

Quantifier elimination algorithm to boolean combination of $\exists\forall$ -formulas in the theory of a free group

Olga Kharlampovich, Alexei Myasnikov

July 24, 2012

Abstract

It was proved by Sela and by the authors that every formula in the theory of a free group F is equivalent to a boolean combination of $\exists\forall$ -formulas. We also proved that the elementary theory of a free group is decidable (there is an algorithm given a sentence to decide whether this sentence belongs to $Th(F)$). In this paper we give an algorithm for reduction of a first order formula over a free group to an equivalent boolean combination of $\exists\forall$ -formulas.

1 Introduction

It was proved in [5],[3] that every formula in the theory of a free group F is equivalent to a boolean combination of $\exists\forall$ -formulas. We also proved that the elementary theory of a free group is decidable (there is an algorithm given a sentence to decide whether this sentence belongs to $Th(F)$). If the language of the free group F contains constants, then it was shown in [1] that every definable subset of F is defined by some boolean combination of formulas

$$\exists X\forall Y(U(P, X) = 1 \wedge V(P, X, Y) \neq 1), \quad (1)$$

where X, Y, P are tuples of variables. We call these formulas *conjunctive $\exists\forall$ -formulas*. We will prove the following result.

Theorem 1. *Let F be a free group. There exists an algorithm given a first-order formula ϕ to find a boolean combination of $\exists\forall$ -formulas that defines the same set as ϕ over F .*

2 Effectiveness of the relative JSJ decomposition

In [4] we proved the following results.

Theorem 2. [4] *There exists an algorithm to obtain a cyclic and abelian JSJ decompositions for a f.g. fully residually free group modulo the subgroup of constants F .*

Theorem 3. ([4], Theorem 13.1, [3], Theorem 35) *There exists an algorithm to obtain an abelian JSJ decomposition for a f.g. fully residually free group modulo finitely generated subgroups K_1, \dots, K_m and to find the maximal standard quotient.*

3 Effectiveness of the global bound in finiteness results

In Section 5.4 of [3] we defined the notion of a sufficient splitting of a group K modulo a class of subgroups \mathcal{K} . Let F be a free group with basis A , $P = A \cup \{p_1, \dots, p_k\}$, $H = \langle P \rangle$. Let \mathcal{K} consist of one subgroup $\mathcal{K} = \{H\}$. Let $K = \langle X, P | S(X, P) \rangle$, and suppose that K does not have a sufficient splitting modulo H . Let D be an abelian JSJ decomposition of K modulo H .

We recall the notion of algebraic solutions. Let K_1 be a fully residually free quotient of the group K , $\kappa : K \rightarrow K_1$ the canonical epimorphism, and $H_1 = H^\kappa$ the canonical image of H in K_1 . An elementary abelian splitting of K_1 modulo H_1 which does not lift into K is called a *new* splitting.

Definition 1. (Definition 20 [3]) *In the notation above the quotient K_1 is called reducing if one of the following holds:*

1. K_1 has a non-trivial free decomposition modulo H_1 ;
2. K_1 has a new elementary abelian splitting modulo H_1 .

We say that a homomorphism $\phi : K \rightarrow K_1$ is *special* if ϕ either maps an edge group of D to the identity or maps a non-abelian vertex group of D to an abelian subgroup.

Let $\mathcal{R} = \{K/R(r_1), \dots, K/R(r_s)\}$ be a complete reducing system for K (see [3]). Now we define algebraic and reducing solutions of $S = 1$ in F with respect to \mathcal{R} . Let $\phi : H \rightarrow F$ be a fixed F -homomorphism and Sol_ϕ the set of all homomorphisms from K onto F which extend ϕ . A solution $\psi \in Sol_\phi$ is called *reducing* if there exists a solution $\psi' \in Sol_\phi$ in the \sim_{MAX} -equivalence class of ψ which satisfies one of the equations $r_1 = 1, \dots, r_k = 1$. All non-reducing non-special solutions from Sol_ϕ are called *K-algebraic* (modulo H and ϕ).

Theorem 4. ([1], Theorem 6) *Let $H \leq K$ be as above. The fact that for parameters P there are exactly N non-equivalent Max-classes of K-algebraic solutions of the equation $S(X, P) = 1$ modulo H can be written as a boolean combination of conjunctive $\exists\forall$ -formulas (these are formulas of type (1)).*

We recall the proof. The generating set X of K corresponding to the decomposition D can be partitioned as $X = X_1 \cup X_2$ such that $G = \langle X_2 \cup P \rangle$

is the fundamental group of the graph of groups obtained from D by removing all QH-subgroups. If c_e is a given generator of an edge group of D , then we know how a generalized fractional Dehn twist (AE-transformation or extended automorphism in the terminology of [3], [2]) σ associated with edge e acts on the generators from the set X . Namely, if $x \in X$ is a generator of a vertex group, then either $x^\sigma = x$ or $x^\sigma = c^{-m}xc^m$, where c is a root of the image of c_e in F , or in case e is an edge between abelian and rigid vertex groups and x belongs to the abelian vertex group, $x^\sigma = xc^m$. Similarly, if x is a stable letter then either $x^\sigma = x$ or $x^\sigma = xc^m$.

One can write elements c_e as words in generators X_2 , $c_e = c_e(X_2)$. Denote $T = \{t_i, i = 1, \dots, m\}$. Consider a formula

$$\exists X_1 \exists X_2 \forall Y \forall T \forall Z (S(X_1, X_2, P) = 1 \wedge \neg \left(\bigwedge_{i=1}^m [t_i, c_i(X_2)] = 1 \wedge Z = X_2^{\sigma_T} \wedge S(Y, X_2, P) = 1 \wedge V(Y, Z, P) = 1 \right)).$$

It says that there exists a solution of the equation $S(X_1, X_2, P) = 1$ that is not Max-equivalent to a solution Y, Z, P that satisfies $V(Y, Z, P) = 1$. If now $V(Y, Z, P) = 1$ is a disjunction of equations defining maximal reducing quotients, then this formula states that for parameters P there exists at least one Max-class of algebraic solutions of $S(X, P) = 1$ with respect to H .

Denote

$$\tau(T, X_2, Y, Z) = \left(\bigwedge_{i=1}^m [t_i, c_i(X_2)] = 1 \wedge Z = X_2^{\sigma_T} \wedge S(Y, X_2, P) = 1 \wedge V(Y, Z, P) = 1 \right)$$

. The following formula states that for parameters P there exists at least two non-equivalent Max-classes of algebraic solutions of $S(X, P) = 1$ with respect to H .

$$\theta_2(P) = \exists X_1, X_3 \exists X_2, X_4 \forall Y, Y' \forall T, T', T'' \forall Z, Z' (S(X_1, X_2, P) = 1 \wedge S(X_3, X_4, P) = 1 \wedge \neg \left(\tau(T, X_2, Y, Z) \vee \tau(T', X_4, Y', Z') \vee \left(\bigwedge_{i=1}^m [t_i'', c_i(X_2)] = 1 \wedge X_2^{\sigma_{T''}} = X_4 \right) \right)).$$

Similarly one can write a formula $\theta_N(P)$ that states for parameters P there exist at least N non-equivalent Max-classes of algebraic solutions of $S(X, P) = 1$ with respect to H .

Then $\theta_N(P) \wedge \neg \theta_{N+1}(P)$ states that there are exactly N non-equivalent Max-classes. The theorem is proved.

Now we will give a simple algorithm to find the global bound in Theorem 11 [3].

Theorem 5. ([3], Theorem 11) *Let H, K be finitely generated fully residually F groups such that $F \leq H \leq K$ and K does not have a sufficient splitting modulo H . Let D be an abelian JSJ decomposition of K modulo H (which may be trivial). There exists a constant $N = N(K, H)$ such that for each F -homomorphism*

$\phi : H \rightarrow \Gamma$ there are at most N algebraic pair-wise non-equivalent with respect to \sim_{AEQ} and, therefore, with respect to \sim_{MAX} , homomorphisms from K to Γ that extend ϕ .

Moreover, the constant N for the number of \sim_{MAX} -non-equivalent homomorphisms can be found effectively.

Proof. We will only prove the effectiveness here. To make presentation easier, we consider first the case when the group K from the formulation of Theorem 11 does not have a splitting modulo H . We consider the formula

$$\exists P \exists Y_1, \dots, Y_m (\wedge_{i=1}^m S(P, Y_i) = 1 \wedge Y_i \neq Y_j (i \neq j) \wedge_{t=1}^k \wedge_{i=1}^m r_t(P, Y_i) \neq 1).$$

We know from Theorem 11 that possible number m of algebraic solutions is bounded. Therefore for some m such a formula will be false. This m can be found because the existential theory of a free group is decidable. Therefore $N = m - 1$.

Now we consider the case when the group K from the formulation of Theorem 11 has a splitting modulo H but not a sufficient splitting. This case is more complicated because we have to write that solutions corresponding to tuples Y_1, \dots, Y_m are not reducing and not in the same \sim_{MAX} equivalence classes for $i \neq j$. This means that there exist no elements representing QH subgroups and no elements commuting with edge groups of the JSJ decomposition of K modulo H such that application of generalized fractional Dehn twists corresponding to these elements take some of these solutions to reducing solutions or take one solution to the other. This fact can be expressed in terms of $\exists\forall$ -sentence that is true if and only if there exists a homomorphism $H \rightarrow F$ that can be extended to m algebraic and not \sim_{MAX} equivalent homomorphisms $K \rightarrow F$. The proof of [3], Theorem 36 and [3], Section 12.1 where the decidability of $\exists\forall$ -theory of a free group is stated does not use Theorem 11. Then the bound on m can be found effectively because we can find for which m the sentence is false and therefore such homomorphism $H \rightarrow F$ does not exist. \square

4 Groups with no sufficient splitting and definable sets

For simplicity we assume that we are working in the language of groups with constants. The proof of Theorem 39 in Section 12.7 of [3] shows that the formula

$$\Phi(P) = \forall Z \exists X \forall Y (U(X, Y, Z, P) = 1 \rightarrow V(X, Y, Z, P) = 1). \quad (2)$$

is false for a value \bar{P} of the variables P if and only if the conjunction of disjunctions of formulas of the two types given below is true for \bar{P} . We will write these formulas in the same form as they appear in Section 12.7 of [3]. Notice that instead of the union of variables X_1, Y_1, \dots, X_{k-1} in these formulas we take variables P .

$$\exists Z_{k-1} \forall B, C (U(P, Z_{k-1}) = 1 \wedge V(P, Z_{k-1}, B, C) \neq 1), \quad (3)$$

$$\forall Z_{k-1} \exists B (U'(P, Z_{k-1}) = 1 \rightarrow V'(P, Z_{k-1}, B) = 1). \quad (4)$$

The first formula is in the form (1). The negation of the second formula is also in the form (1).

We will look in more detailed way to the procedure to obtain formulas (3) and (4) in [3] and show that there is an algorithm for each step of the procedure.

The set of specializations P such that formula (2) is false in F is associated with a finite number of groups without sufficient splitting modulo $H = \langle P \rangle$ and for each such group K with a given combination of Max-classes of algebraic solutions. The total number of such classes is bounded and there is an algorithm to find this bound by Theorem 5.

We will recall now how formulas (3),(4) appear in [3]. We will repeat the construction from [3] with slightly changed notation. Instead of variables X_1, Y_1, \dots, X_{k-1} in Section 12 in [3] we now have parameters P . It will also be more convenient to consider instead of formula (2) the negation of such formula

$$\neg \Phi(P) = \exists Y_{k-1} \forall X_k \exists Y_k (U(P, X_{k-1}, X_k, Y_k) = 1 \wedge V(P, Y_{k-1}, X_k, Y_k) \neq 1). \quad (5)$$

To obtain effective quantifier elimination to boolean combinations of $\exists \forall$ -formulas it is enough to give an algorithm to find such a boolean combination that defines a set defined by $\neg \Phi(P)$.

For every \bar{P} for which $\neg \Phi(\bar{P})$ is true, there exists some \bar{Y}_{k-1} and (by the Merzljakov theorem) a solution $Y_k = f(X_k, A)$ of $U = 1 \wedge V \neq 1$ in $F(X_k) * F(A)$. All such solutions for all possible values of P belong to a finite number of fundamental sequences with terminal groups $F_{R(U_{1,i})} * F(X_k)$, where $U_{1,i} = U_{1,i}(P, Y_{k-1}, Y_{k-1}^{(1)})$ and $F_{R(U_{1,i})}$ is a group with no sufficient splitting modulo $\langle P, Y_{k-1} \rangle$ (see Section 12.2, [3]). These groups can be effectively found by Theorem 3.

We now consider each of these fundamental sequences separately. Those values P, Y_{k-1} for which there exist a value of X_k such that the equation $V(P, Y_{k-1}, X_k, f(X_{k-1}, Y_{k-1}^{(1)}, P)) = 1$ is satisfied for any function f give a system of equations on $F_{R(U_{1,i})} * F(X_k)$. This system is equivalent to a finite subsystem (to one equation in the case when we consider formulas with constants). Let G be the coordinate group of this system and $G_i, i \in J$ be the corresponding fully residually free groups.

We introduced in Section 12.2, [3], the tree $T_{X_k}(G)$ which is constructed the same way as $T_{EA}(G)$ with X_k, Y_k considered as variables and $P, Y_{k-1}, Y_{k-1}^{(1)}$ as parameters. To each group G_i we assign fundamental sequences modulo $\langle P, Y_{k-1}, Y_{k-1}^{(1)} \rangle$. Their terminal groups are groups $F_{R(V_{2,i})}$, where

$$V_{2,i} = V_{2,i}(P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(2)})$$

that do not have sufficient splitting modulo $\langle P, Y_{k-1}, Y_{k-1}^{(1)} \rangle$. Then we find all formula solutions Y_k of the conjunction

$$U(P, X_{k-1}, X_k, Y_k) = 1 \wedge V(P, Y_{k-1}, X_k, Y_k) \neq 1$$

in the corrective normalizing extensions of the NTQ groups corresponding to these fundamental sequences for X_k (see [2], Theorem 12). These formula solutions Y_k are described by a finite number of fundamental sequences with terminal groups $F_{R(U_{2,i})}$, where $U_{2,i} = U_{2,i}(P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(2)}, Y_{k-1}^{(2)})$. Then again we investigate the values of X_k that make the word $V(P, Y_{k-1}, X_k, Y_k)$ equal the identity for all these formula solutions Y_k . And we continue the construction of $T_{X_k}(G)$. We can prove that this tree is finite exactly the same way as we proved the finiteness of the $\exists\forall$ -tree. We will call $T_{X_k}(G)$ *the parametric $\exists\forall$ -tree* for the formula $\neg\Psi(P)$. For each branch of the tree T_{X_k} we assign a sequence of groups

$$F_{R(U_{1,i})}, F_{R(V_{2,i})} \cdots, F_{R(V_{r,i})}, F_{R(U_{r,i})}$$

as in [3], Section 12.2. Corresponding irreducible systems of equations are:

$$\begin{aligned} U_{1,i} &= U_{1,i}(P, Y_{k-1}, Y_{k-1}^{(1)}), \\ U_{m,i} &= U_{m,i}(P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(m)}, Y_{k-1}^{(m)}), \quad m = 2, \dots, r, \end{aligned}$$

which correspond to the terminal groups of fundamental sequences describing Y_k of level $(m, m-1)$, and

$$V_{m,i} = V_{m,i}(P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(m)}), \quad m = 2, \dots, r$$

which correspond to the terminal groups of fundamental sequences describing X_k of level (m, m) . They correspond to vertices of T_{X_k} that have distance m to the root.

For each m the group $F_{R(U_{m,i})}$ does not have a sufficient splitting modulo the subgroup $\langle P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(m)} \rangle$, and the group $F_{R(V_{m,i})}$ does not have a sufficient splitting modulo the subgroup generated by $P, Y_{k-1}, Y_{k-1}^{(1)}$.

On each step we consider terminal groups of all levels. Below we will sometimes skip index i and write U_m, V_m instead of $U_{m,i}, V_{m,i}$.

There is a list of algorithmic problems that we can solve for fully residually free groups in [3], Section 8. The construction of the relative JSJ decomposition and canonical fundamental sequences modulo a finite number of finitely generated subgroups is effective by Theorem 3. By Theorem 27, [3], given a fully residually free group G , a splitting D of G , and a freely indecomposable finitely generated subgroup H of G defined by a finite generating set Y , one can effectively find a splitting D_H of H induced from D . Moreover, one can describe all the vertex and edge groups which occur in D_h explicitly as words in generators Y .

Proposition 1. 1. *The complete system of reducing quotients of a group with no sufficient splitting modulo a subgroup can be found effectively.*

2. *There is an algorithm to construct the finite parametric $\exists\forall$ -tree T_{X_k} , for each branch of the tree T_{X_k} a finite family of groups*

$$F_{R(U_{1,i})}, F_{R(V_{2,i})} \cdots, F_{R(V_{r,i})}, F_{R(U_{r,i})},$$

and for each vertex a fundamental sequence describing either Y_k (if the associated group is $F_{R(U_{j,i})}$) or X_k (if the associated group is $F_{R(V_{j,i})}$).

Proof. 1. The complete system of reducing quotients of a group with no sufficient splitting modulo a subgroup can be found effectively ([3], Lemma 20).

2. This uses the algorithm to construct a complete system of reducing quotients and the fact that we can construct fundamental sequences modulo a finite set of finitely generated subgroups algorithmically. \square

The tree T_{X_k} is finite, we can have schemes of levels $(1, 0)$, $(1, 1)$, $(2, 1)$, $(2, 2)$ etc up to some number (m, m) .

Let G be a finitely generated group. Recall that any family of homomorphisms $\Psi = \{\psi_i : G \rightarrow F\}$ factors through a finite set of maximal fully residually free groups H_1, \dots, H_k that all are quotients of G . We first take a quotient G_1 of G by the intersection of the kernels of all homomorphisms from Ψ , and then construct maximal fully residually free quotients H_1, \dots, H_k of G_1 . We say that Ψ discriminates groups H_1, \dots, H_k , and that each H_i is a fully residually free group discriminated by Ψ .

We will concentrate on level $(2, 1)$ now. In Definition 27 and Definition 28 [3] we define initial fundamental sequences of levels $(2, 1)$ and $(2, 2)$ and width i (the possible width is bounded) modulo P . Since we are now considering the formula $\neg\Psi$ instead of Ψ , we will slightly change the definition here. It will be more convenient to replace condition (6) from Definition 28 by its negation and add this negation on level $(2, 1)$.

Definition 2. Let $F_{R(V_{2,1})}, \dots, F_{R(V_{2,t})}$ be the whole family of groups on level $(1, 1)$. To construct the initial fundamental sequences of level $(2, 1)$ and width $i = i_1 + \dots + i_t$, we consider the fundamental sequences modulo the subgroup $\langle P \rangle$ for the groups discriminated by i solutions of the systems

$$U_{2,m_s}(P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(2,j,s)}, Y_{k-1}^{(2,j,s)}) = 1, \quad j = 1, \dots, i_s, \quad s = 1, \dots, t,$$

with properties:

- (1) $Y_{k-1}^{(1)}, Z_{k-1}^{(2,j,s)}, Y_{k-1}^{(2,j,s)}$ are algebraic;
- (2) $Z_{k-1}^{(2,j,s)}$ are not MAX-equivalent to $Z_{k-1}^{(2,p,s)}$, $p \neq j$, $p, j = 1, \dots, i_s$, $s = 1, \dots, t$;
- (3) for any of the finite number of values of $Z_{k-1}^{(2)}$ fundamental sequences for $V_{2,s}(P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(2)}) = 1$ are contained in the union of fundamental sequences for $U_{2,m_s}(P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(2,j)}, Y_{k-1}^{(2,j)}) = 1$ for different values of $Y_{k-1}^{(2,j,s)}$;
- (4) there is no non-equivalent $Z_{k-1}^{(2,i_s+1,s)}$ algebraic solving $V_{2,s} = 1$, $s = 1, \dots, t$.
- (5) the solution $P, Y_{k-1}, Y_{k-1}^{(1)}$ does not satisfy a proper equation which implies $V = 1$ for any value of X_k .

(6) for any s the solution $P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(2,1,s)}, Y_{k-1}^{(2,1,s)}$ can not be extended to a solution of some

$$V_{3,s}(X_1, Y_1, \dots, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(2,1,s)}, Y_{k-1}^{(2,1,s)}, Z_{k-1}^{(3,1,s)}) = 1.$$

We call this group a configuration group. We also call a tuple

$$Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(2,j,s)}, Y_{k-1}^{(2,j,s)}, j = 1, \dots, i_s, s = 1, \dots, t$$

satisfying the conditions above a certificate for $\neg\Psi$ for P (of level $(2,1)$, width i and depth 1). We add to the generators of the configuration group additional variables Q for the primitive roots of a fixed set of elements for each certificate (these are primitive roots of the images of the edge groups and abelian vertex groups in the relative JSJ decompositions of the groups $F_{R(V_{2,1})}$).

Proposition 2. Let $H = F_{R(W)}$ be one of the configuration groups with generators

$$P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(2,j,s)}, Y_{k-1}^{(2,j,s)}, j = 1, \dots, i_s, s = 1, \dots, t, Q.$$

Then there is an algorithm to find each terminal group of each fundamental sequence for H modulo P .

Proof. As in the proof of Theorem 11, [3] we extensively use the technique of generalized equations described in [2], Subsection 4.3 and Section 5. The reader has to be familiar with these sections of [2]. In the proof of Theorem 11, [3] we show how to construct given a group K that does not have a sufficient splitting modulo a subgroup H a finite system of cut equations Π (see [2], Section 7.7) for a minimal in its Max-class solution such that the intervals of Π are labeled by values of the generators of H . For each system

$$U_{2,m_s}(P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(2,j,s)}, Y_{k-1}^{(2,j,s)}) = 1$$

we construct a cut equation modulo parameters subgroup $\langle P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(2,j,s)} \rangle$. The intervals of this cut equation are labeled by $P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(2,j,s)}$. For the intervals labeled by $P, Y_{k-1}, Y_{k-1}^{(1)}$ we add a cut equation for the system

$$V_{2,m}(P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(2,j,s)}) = 1$$

modulo the parameters subgroup $\langle P, Y_{k-1}, Y_{k-1}^{(1)} \rangle$. For the intervals labeled by P, Y_{k-1} we add cut equations for the system

$$U_{1,m}(P, Y_{k-1}, Y_{k-1}^{(1)}) = 1$$

modulo the parameters subgroup $\langle P, Y_{k-1} \rangle$. The intervals labeled by P will be the same for all these cut equations. Similarly we identify all the intervals labeled by the same variables that occurs in different cut equations. We now add to the obtained cut equation, which can be also considered as a generalized

equation, the inequalities that guarantee that conditions (1)-(6) are satisfied. These inequalities are just saying that specializations of variables corresponding to some sub-intervals of the generalized equation must not be identities. But this is a standard requirement for a solution of a generalized equation. For example, we write an equation $r_1(Z_{k-1}^{(2,j)}) = \lambda_1$ and say that λ_1 is a base of the generalized equation. Then the condition $\lambda_1 \neq 1$ must be automatically satisfied for a solution of a generalized equation. So we can construct a finite number of generalized equations such that each certificate corresponding to minimal in their Max-classes specializations is a solution of one of these generalized equations \mathcal{GE} .

We now construct fundamental sets of solutions of the equations \mathcal{GE} modulo $\langle P \rangle$. Notice that not all solutions from the fundamental set satisfy the necessary inequalities, but if we restrict the sets of automorphisms on all the levels to those whose application preserves corresponding generalized equations, we will have solutions of inequalities too. Therefore, a generic family of solutions does satisfy the inequalities. Using our standard procedure we construct fundamental sequences induced by the subgroup with generators

$$P, Y_{k-1}, Y_{k-1}^{(1)}, Z_{k-1}^{(2,j,s)}, Y_{k-1}^{(2,j,s)} j = 1, \dots, i_s, s = 1, \dots, t, Q.$$

Terminal groups of these fundamental sequences are precisely the groups we are looking for. \square

This implies the following result.

Corollary 1. *There is an algorithm to construct the initial fundamental sequences for Y_{k-1} of level $(2,1)$ and width i related to $F_{R(V_2)}$.*

Lemmas 27, [3], states that the set of parameters P for which there exists a fundamental sequence of level $(2,1)$ and width i and a certificate, consists of those P for which there exists a generic family of certificates (*generic certificate*) and those for which all the certificates factor through a proper projective image of this fundamental sequence. Actually, Lemma 27 deals with certificates satisfying only properties (1)-(5), but the proof does not change if we add property (6) to the definition of a certificate.

For a given value of P the formula $\neg\Psi$ can be proved on level $(2,1)$ and depth 1 if and only if the following conditions are satisfied.

- (a) There exist algebraic solutions for some $U_{i,coeff} = 1$ corresponding to the terminal group of a fundamental sequence $V_{i,fund}$ for a configuration group modulo P .
- (b) These solutions do not factor through the fundamental sequences that describe solutions from $V_{i,fund}$ that do not satisfy one of the properties (1)-(6). There is a finite number of such fundamental sequences.
- (c) These solutions do not factor through the terminal groups of fundamental sequences of level $(2,1)$ and greater depth derived from $V_{i,fund}$.

- (d) $(X_1, Y_1, \dots, Y_{k-1}, Y_{k-1}^{(1)})$ cannot be extended to a solution of $V = 1$ by arbitrary X_k (X_k of level 0) and Y_k of level $(1,0)$.

In this case there is a generic certificate of level $(2,1)$ width i and depth 1. These conditions can be described by a boolean combination of conjunctive $\exists\forall$ -formulas of type (1). Similarly we consider fundamental sequences of level $(2,1)$ width i and depth 2 and deeper fundamental sequences of level $(2,1)$ width i . We construct the projective tree (see [3], Section 11) to construct these deeper sequences. We now need another algorithmic result that states that the main technical tool of the procedure of constructing the projective tree, tight enveloping NTQ groups and fundamental sequences, can be effectively constructed. We also consider similarly fundamental sequences of levels $(m, m-1)$

Proposition 3. 1. *Given a fully residually free group $G = F_{R(U)}$, the canonical NTQ system $W = 1$ corresponding to a branch of the canonical embedding tree $T_{CE}(F_{R(U)})$ of the system $U = 1$, a system of equations $\mathcal{P} = 1$ with coefficients in $F_{R(W)}$ having a solution in some extension of $F_{R(W)}$, there is an algorithm for the construction of tight enveloping NTQ groups and fundamental sequences (they are defined in [3], Section 11.2).*

2. *The bound in Lemma 28 from [3] can be found effectively.*

Proof. 1. The first algorithm can be constructed using [3], Theorems 26 and 27.

2. The bound in Lemma 28 from [3] can be found effectively as in Theorem 5.

We now can make all the steps of the quantifier elimination procedure (to boolean combination of formulas (1)) algorithmically. This proves Theorem 1. \square

References

- [1] O. Kharlampovich and A. Myasnikov, Definable sets in a hyperbolic group.
- [2] O. Kharlampovich and A. Myasnikov, Implicit function theorem over free groups, *Journal of Algebra*, vol 290/1, pp. 1–203, 2005.
- [3] O.Kharlampovich, A. Myasnikov, *Elementary theory of free non-abelian groups*. *Journal of Algebra*, 2006, Volume 302, Issue 2, p. 451-552.
- [4] O. Kharlampovich, A. Myasnikov, Effective JSJ decompositions. *Group Theory: Algorithms, Languages, Logic*, Contemp. Math., AMS (Borovik, editor), CONM/378, 87-212, 2005.
- [5] Z. Sela, Diophantine geometry over groups. V1. Quantifier elimination. I. *Israel J. Math.* 150 (2005), 1197.